PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-183641**
(43)Date of publication of application : **28.06.2002**

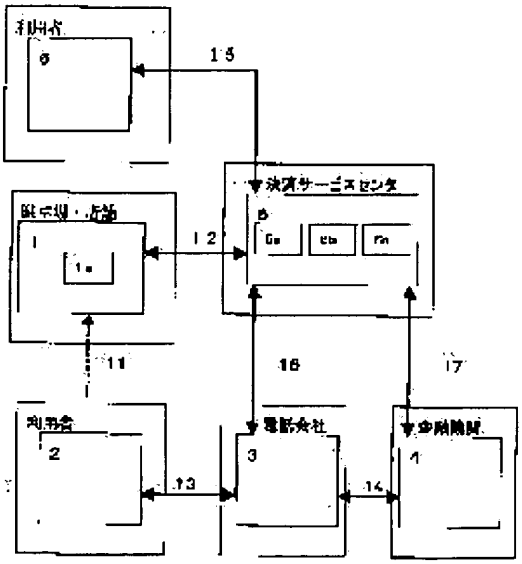
(51)Int.CI. G06F 17/60

(21)Application number : **2000-385706**
(22)Date of filing : **19.12.2000**

(71)Applicant : **SUMITOMO CORP**
CHUSHAJO SOGO
KENKYUSHO:KK
(72)Inventor : **SHIGEMATSU ATSUSHI**
OGITA TAKEYUKI
ISOBE TOSHIYA
MORI FUSAO
ISHIKAWA KOJI
OSHIMA TASUKU
KOJIMA MASAO

(54) PRINCIPAL CONFIRMING METHOD AND SYSTEM USING PORTABLE TERMINAL

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a principal confirming method and a principal confirming system required in cashless settlement of a service charge, such as the use of a parking garage, shopping and a mail-order sale in a store, and use of Internet ASP.
SOLUTION: This principal authenticating method required in the cashless settlement, comprises a procedure (a step 1) for informing a control device arranged in a providing site of commodity and service of a telephone number of a portable information terminal possessed by a user, a procedure (a step 2) for informing a settlement control device of the telephone number of the information terminal from a control device, a procedure (a step 3) for inquiring whether to approve to perform settlement by presenting a demand cause and the amount by telephoning to the information terminal of the telephone number from the settlement control device, and a procedure (a step 4) for confirming the principal, by confirming the input of the effect of approving the perform the settlement.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the

examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－183641
（P2002－183641A）
(43)公開日　平成14年６月28日(2002.6.28)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60	４１４ ＺＥＣ ５０６	Ｇ０６Ｆ　17/60	４１４ ＺＥＣ ５０６	５Ｂ０４９

審査請求　未請求　請求項の数10　ＯＬ　（全 17 頁）

(21)出願番号　特願2000－385706(P2000－385706)

(22)出願日　平成12年12月19日(2000.12.19)

(71)出願人　000002129
住友商事株式会社
東京都中央区晴海一丁目８番11号

(71)出願人　598121606
株式会社駐車場綜合研究所
東京都渋谷区宇田川町２番１号　渋谷ホームズ1205号

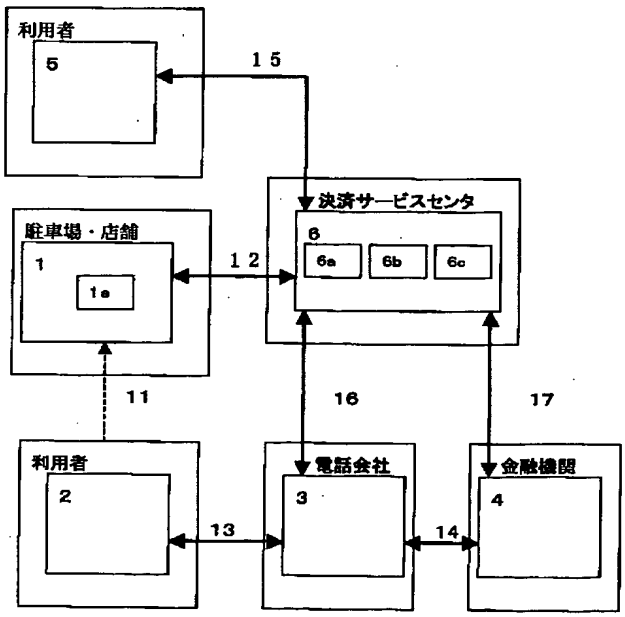
(72)発明者　重松　篤
愛知県名古屋市昭和区丸屋町６－67

(74)代理人　100085028
弁理士　西森　浩司

最終頁に続く

(54)【発明の名称】　携帯端末を利用した本人確認方法及びシステム

(57)【要約】
【課題】　駐車場利用や店舗での買物や通信販売、インターネットＡＳＰ利用などの利用料金の非現金決済において必要となる本人確認方法及び本人確認システムを提供する。
【解決手段】　非現金決済において必要となる本人認証方法であって、商品・サービスの提供サイトに設けられた管理装置に利用者の所持する携帯可能な情報端末の電話番号を通知する手順(ステップ１)と、管理装置から決済管理装置に、情報端末の電話番号を通知する手順(ステップ２)と、決済管理装置から当該電話番号の情報端末に電話を掛け、請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う手順(ステップ３)と、決済を行うことを許諾する旨の入力を確認することにより本人確認を取る手順(ステップ４)とを含んで構成されている。



1

【特許請求の範囲】

【請求項1】駐車場利用や店舗での買物や通信販売、インターネットＡＳＰ利用などの利用料金の非現金決済において必要となる本人認証方法であって、商品・サービスの提供サイトに設けられた管理装置に少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順と、前記管理装置から決済サービスセンタに設けられた決済管理装置に、少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順と、前記決済管理装置から当該電話番号の情報端末に電話を掛け、少なくとも請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う手順と、そして、前記情報端末から決済を行うことを許諾する旨の入力を確認することにより、非現金決済において必要となる本人認証を行う手順と、を含んで構成されてなる本人確認方法。

【請求項２】請求項１に記載の本人確認方法において、本人確認を取る手順は、携帯可能な情報端末の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末の契約者のみが知り得る個人情報のいずれか1つ又は複数と組み合わせて使用する手順からなることを特徴とする本人確認方法。

【請求項３】請求項１又は２に記載の本人確認方法において、利用者から前記管理装置への通知手順は、利用者が管理装置に設けられた入力装置を用いて直接入力する、利用者が所持している携帯可能な情報端末から無線通信により非接触入力する、又は、利用者が有するインターネット等の通信回線に接続可能な第二情報端末から電話回線などの通信回線を介して入力する手順からなることを特徴とする本人確認方法。

【請求項４】請求項１又は２に記載の本人確認方法において、本人確認を取る手順は、利用者が管理装置から入力する自由な暗証番号と、利用者が所持している携帯可能な情報端末から入力する自由な暗証番号を決済管理装置で照合・確認する手順からなることを特徴とする本人確認方法。

【請求項５】請求項１又は２に記載の本人確認方法において、本人確認を取る手順は、管理装置が自動的に発行するランダムな暗証番号を携帯可能な情報端末にて提示し、利用者が管理装置から入力するランダムな暗証番号を決済管理装置で照合・確認する手順からなることを特徴とする本人確認方法。

【請求項６】駐車場利用や店舗での買物や通信販売、インターネットＡＳＰ利用などの利用料金の非現金決済において必要となる本人認証システムにおいて、電話機能を持った携帯可能な情報端末と、商品・サービスの提供サイトに設けられ、利用者から入力された少なくとも利用者の所持する携帯可能な情報端末の電話番号を決済管理装置に通知する電話番号通知手段を有してなる管理装置と、携帯可能な情報端末及び管理装置に公衆電話回線等の通信回線を用いて接続され決済サービスセンタに設けられた決済管理装置であって、管理装置から通知された利用者の所持する携帯可能な情報端末の電話番号に基づいて当該電話番号の情報端末に電話を掛け、少なくとも請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う決済許諾問合せ手段と、利用者の有する携帯可能な情報端末から決済を行うことを許諾する旨の入力を確認することにより非現金決済において必要となる本人確認手段とを有してなる決済管理装置と、を含み構成されてなる本人確認システム。

【請求項７】請求項６に記載の本人確認システムにおいて、前記決済管理装置の本人確認手段は、携帯可能な情報端末の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等の携帯可能な情報端末の契約者のみが知り得る個人情報のいずれか1つ又は複数と組み合わせて本人確認するようにしてなることを特徴とする本人確認システム。

【請求項８】請求項６又は７に記載の本人確認システムにおいて、前記管理装置は、利用者が直接必用事項を入力することができる入力装置、利用者が所持している携帯可能な情報端末から無線通信により非接触入力することができる受信装置、又は、利用者が有するインターネット等の通信回線に接続可能な第二情報端末から電話回線などの通信回線を介して入力された入力信号を変換する入力信号変換装置のいずれか又はそれらの任意の組み合わせを含んでなることを特徴とする本人確認システム。

【請求項９】請求項６又は７に記載の本人確認システムにおいて、前記決済管理装置の本人確認手段は、利用者が管理装置から入力する自由な暗証番号と、利用者が所持している携帯可能な情報端末から入力する自由な暗証番号とを照合・確認するようにしてなることを特徴とする本人確認システム。

【請求項１０】請求項６又は７に記載の本人確認システムにおいて、前記決済管理装置の本人確認手段は、管理装置が自動的に発行するランダムな暗証番号を携帯可能な情報端末にて提示し、利用者が管理装置から入力するランダムな暗証番号を決済管理装置で照合・確認するようにしてなることを特徴とする本人確認システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】駐車場利用や店舗での買物や通信販売、インターネットＡＳＰ利用などの利用料金の非現金決済において必要となる本人確認方法及び本人確認システムに係り、特に、多くの日本人が所持している携帯可能な情報端末の電話会社による信用力の有る認証

を各種の非現金決済において必要となる本人であることの確認に利用した本人確認方法及び本人確認システムに関する。

【０００２】

【従来の技術】駐車場や店舗や通信販売やインターネットのＡＳＰなどの利用料金を支払う場合、各種の方法が存在していた。

１）　現金での支払は、最も単純で金銭の授受という点では最も確実な方法である。また、通信販売においては、代金引換えや商品受け取り後に郵便為替等による支払も行われていた。

２）　クレジットカードによる支払では、当該カードを商品・サービスの提供サイトに設けられたカードリーダ（読取機）に通し磁気ストリップに記録された暗証番号等を読み取り、一方、利用者に暗証番号を言わせて照合する。かかる照合により本人であることを確かめた後（本人確認後）、当該取引についての決済を行う。カードリーダの無い場合には、カード裏面に設けられたサイン欄に記述のサインとの照合により確認を行う。

【０００３】３）　デビットカードでは、金融機関のキャッシュカードを使って、小売店での買い物時に利用者の預金口座から代金を引き落とし、小売店が指定した口座に入金する。クレジットが与信枠を設けるのに対し、デビットは即時決済を行う点で相違している。デビットカード利用者が本人であることの確認は、クレジットカードと同様で、カードリーダ（読取機）によるか、サインの照合によって行っている。消費者にとっては、現金を持たずに買い物できる上に即時決済できるという利便性がある。一方、小売店にとっては、クレジットカードよりも安い手数料で即時に売上金が回収できる利点がある。

４）　プリペイドカードによる支払方法では、利用者がそのカードを購入した本人であるか否かは問わず、カードに記述された残高から利用した分だけ差し引き、利用可能な金額を更新する。小銭が不要で決済が短時間で済む、割引やプレミアム、カードデザインのファッション性等により普及が促進されている。最近は、パスネット等1枚のカードで複数の鉄道、バスを利用できるものが発行されて人気を集めている。

【０００４】５）　一風変わった支払方法としては、ダイヤルＱ２がある。ダイヤルＱ２では、利用者が自己の電話機能を持った情報端末を使用し、この情報端末から情報が登録されているサービス提供会社に電話をかけ利用する。この場合の料金は、利用した情報量により課金される。すなわち、電話会社がサービス提供会社に代行して情報端末を所有する利用者から、具体的には、その電話番号の電話料金と一緒に利用料金の徴収を行っていた。この場合、サービス提供会社により提供される情報を利用する者が当該情報端末の所有者であるか否かは、暗証番号の照合程度の簡単な確認により行っているにし過ぎなかった。

６）　営業などのビジネスにおいて、ＰＣやＰＤＡなどの携帯端末からデータサーバへアクセスした場合の使用料金は、利用者が誰であるかの認証を行った上で予め定めてあった支払方法に従って決済する。この場合の認証は、付属の装置を付けるなど改造が必要である。

【０００５】

【発明が解決しようとする課題】前述した第一の支払方法は、現金をいつも持ち歩かなければならない関係から落としたり盗難にあう危険がつきまとう。また、駐車場の場合のように小銭が無い場合には利用できな。また、雨の日には濡れて紙幣が使えなくなるなどの欠点があった。さらに、代金引換えや郵便為替による支払は、その時に現金の持ち合わせがないと商品を受け取れない。また、郵便局に行って所定の手続きをしなければならない煩わしさが有る。

【０００６】かかる事情により現金を用いない支払方法の開発が要望されていた。かかる要望に応えたものが前記２）～４）であるが、クレジットカード及びデビットカードによる支払は、盗難や拾い物によって入手した第三者が不正使用した場合に大きな被害をもたらす恐れがある。従って、そのカードを使用しようとする者が、カード所有者本人であることを確かめること、すなわち、本人確認を取ることが重要な事項となる。

【０００７】従来、本人であることの確認は、カード裏面の磁気ストリップに記録された暗証番号と利用者が言った暗証番号との照合、又は、カード裏面に設けられたサイン欄に記述のものと利用者が利用明細書に記載したサインとの照合により行っていた。前者の方法では、磁気ストリップに記録された事項を読み取ることができる機器の登場により不正使用に太刀打ちすることができなくなった。かかる欠点を無くし且つカードに蓄積できる情報量を増大したものとしてＩＣチップを埋め込んだクレジットカードも誕生している。しかしながら、価格の点で実用化に至っていない。後者の方では、海外で使用された場合を除いて、サインを真似て練習されると本物と見分けがつかないというのが実情であった。

【０００８】プリペイドカードは、利用者が事業者に与信を与える関係となり、代金後払いのクレジットカードの場合と逆である。プリペイドカードに割引やプレミアムが設定される所以である。その関係から、高額のものの購入には不向きで汎用性に欠ける欠点があった。利用時に本人確認が行われない関係から、盗難や落し物をした場合には回収不可能となっていた。なお、プリペイドカードは、販売した時点で事業者が所期の利益を得てしまうため、利用者保護のための認証システムの構築には不熱心である事情がある。

【０００９】ダイヤルＱ２は、公衆回線等の通信回線を用いて利用者がサービス提供会社に電話をかけ情報を利用した場合に、情報量に応じた利用料金を電話会社がサ

ービス提供会社に代わって徴収する。電話会社は、当該情報の利用に関連して公衆回線を利用したことに対する利用料金を、当該情報端末の契約者を発信者情報を入手することにより特定して徴収する。これにより、利用料金徴収の効率化が図れる。しかしながら、ダイヤルＱ２は、クレジットカードの場合と同様に、暗証番号の照合程度の簡単な確認により利用可能である。従って、暗証番号が漏れた場合等における不正使用に対しては実質的に対処不能である欠点があった。ＰＣやＰＤＡなどの携帯端末からデータサーバへアクセスした場合の使用料金は、利用者が誰であるかの認証を行った上で予め定めてあった支払方法に従って決済する。この場合の認証は、付属の装置を付けることによって確実に行われるが、付属装置の価格が比較的高価である欠点があった。

【００１０】よって、本発明は、多くの日本人が所持している携帯可能な情報端末の電話会社による信用力の有る認証を各種の非現金決済において必要となる本人であることの確認に利用した本人確認方法及び本人確認システムを提供することを目的とする。本発明は、また、本人確認の精度を向上させることができる本人確認方法及び本人確認システムを提供することを目的とする。本発明は、さらに、適宜の手法で携帯可能な情報端末の電話番号を管理装置に通知することができる本人確認方法及び本人確認システムを提供することを目的とする。本発明は、さらにまた、簡単な構成により本人確認の精度を向上させることができる本人確認方法及び本人確認システムを提供することを目的とする。本発明は、さらにまた、簡単な構成により本人確認の精度を向上させることができる他の本人確認方法及び本人確認システムを提供することを目的とする。本発明は、さらにまた、簡単な構成により本人が商品・サービスの提供サイトなど、その場所から入力することを特定する本人確認方法及び本人確認システムを提供することを目的とする。

【００１１】

【発明が解決しようとする手段】本発明は、上述した目的を達成したもので、駐車場利用や店舗での買物や通信販売、インターネットＡＳＰ利用などの利用料金の非現金決済において必要となる本人認証方法であって、商品・サービスの提供サイトに設けられた管理装置に利用者から少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順と、管理装置から決済サービスセンタに設けられた決済管理装置に、少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順と、決済管理装置から当該電話番号の情報端末に電話を掛け、少なくとも請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う手順と、そして、情報端末から決済を行うことを許諾する旨の入力を確認することにより、非現金決済において必要となる本人認証を行う手順とを含んで構成されてなる本人確認方法を提供する。

【００１２】請求項２に記載の発明は、請求項１に記載の本人確認方法において、本人確認を取る手順は、携帯可能な情報端末の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末の契約者のみが知り得る個人情報のいずれか1つ又は複数と組み合わせて使用する手順からなることを特徴とする。請求項３に記載の発明は、請求項１又は２に記載の本人確認方法において、利用者から管理装置への通知手順が、利用者が管理装置に設けられた入力装置を用いて直接入力する、利用者が所持している携帯可能な情報端末から無線通信により非接触入力する、又は、利用者が有するインターネット等の通信回線に接続可能な第二情報端末から電話回線などの通信回線を介して入力する手順からなることを特徴とする。

【００１３】請求項４に記載の発明は、請求項１又は２に記載の本人確認方法において、本人確認を取る手順が、利用者が管理装置から入力する自由な暗証番号と、利用者が所持している携帯可能な情報端末から入力する自由な暗証番号を決済管理装置で照合・確認する手順からなることを特徴とする。請求項５に記載の発明は、請求項１又は２に記載の本人確認方法において、本人確認を取る手順が、管理装置が自動的に発行するランダムな暗証番号を携帯可能な情報端末にて提示し、利用者が管理装置から入力するランダムな暗証番号を決済管理装置で照合・確認する手順からなることを特徴とする。

【００１４】本発明の第二の態様は、駐車場利用や店舗での買物や通信販売、インターネットＡＳＰ利用などの利用料金の非現金決済において必要となる本人であることの確認を取る本人確認システムにおいて、電話機能を持った携帯可能な情報端末と、商品・サービスの提供サイトに設けられ、利用者から入力された少なくとも利用者の所持する携帯可能な情報端末の電話番号を決済管理装置に通知する電話番号通知手段を有してなる管理装置と、携帯可能な情報端末及び管理装置に公衆電話回線等の通信回線を用いて接続され決済サービスセンタに設けられた決済管理装置であって、管理装置から通知された利用者の所持する携帯可能な情報端末の電話番号に基づいて当該電話番号の情報端末に電話を掛け、少なくとも請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う決済許諾問合せ手段と、利用者の有する携帯可能な情報端末から決済を行うことを許諾する旨の入力を確認することにより非現金決済において必要となる本人であることの確認を取る本人確認手段とを有してなる決済管理装置とを含み構成されてなる本人確認システムを提供する。

【００１５】請求項７に記載の発明は、請求項６に記載の本人確認システムにおいて、決済管理装置の本人確認手段は、携帯可能な情報端末の電話登録暗証番号、氏

名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末の契約者のみが知り得る個人情報のいずれか1つ又は複数と組み合わせて本人確認するようにしてなることを特徴とする。

【００１６】請求項８に記載の発明は、請求項６又は７に記載の本人確認システムにおいて、管理装置は、利用者が直接必用事項を入力することができる入力装置、利用者が所持している携帯可能な情報端末から無線通信により非接触入力することができる受信装置、又は、利用者が有するインターネット等の通信回線に接続可能な第二情報端末から電話回線などの通信回線を介して入力された入力信号を変換する入力信号変換装置のいずれか又はそれらの任意の組み合わせを含んでなることを特徴とする。請求項９に記載の発明は、請求項６又は７に記載の本人確認システムにおいて、決済管理装置の本人確認手段は、利用者が管理装置から入力する自由な暗証番号と、利用者が所持している携帯可能な情報端末から入力する自由な暗証番号とを照合・確認するようにしてなることを特徴とする。

【００１７】請求項１０に記載の発明は、請求項６又は７に記載の本人確認システムにおいて、決済管理装置の本人確認手段は、管理装置が自動的に発行するランダムな暗証番号を携帯可能な情報端末にて提示し、利用者が管理装置から入力するランダムな暗証番号を決済管理装置で照合・確認するようにしてなることを特徴とする。

【００１８】

【発明の実施の形態】以下、図面を用いて本発明の本人確認方法及び本人確認システムを詳細に説明する。図１９は、本発明に係る本人確認システムの一実施形態のブロック図である。図１９に示すように、本人確認システムの一実施形態は、概略的に、携帯電話等の電話機能を持った携帯可能な情報端末２と、商品・サービスの提供サイトに設けられた管理装置１と、そして、管理装置1及び情報端末２に公衆電話回線等の通信回線を用いて接続された決済管理装置６とを備えて構成されている。利用者は、管理装置1にある入力装置、例えば、テンキーや画面の数字部位を押圧することにより少なくとも利用者の所持する情報端末２の電話番号を入力することができる。管理装置1は、当該電話番号をメモリに記録すると共に決済管理装置６に通知する。これらの操作は、管理装置1に設けられた電話番号通知手段１ａによって行われる。

【００１９】決済管理装置６は、本システムを維持/管理する決済サービスセンタに設けられるもので、管理装置１から通知された利用者の所持する携帯可能な情報端末２の電話番号に基づいて当該電話番号の情報端末に電話を掛ける制御手段６ａを備えている。決済管理装置６は、また、情報端末２の表示画面に少なくとも請求原因、例えば、ＸＸ駐車場における駐車料金であるとかＯＯデパートにおける買い物であるとかの表示とその金額を提示して決済を行うことを許諾するか否かの問合せを行う決済許諾問合せ手段６ｂと、そして、利用者の有する携帯可能な情報端末２から決済を行うことを許諾する旨の入力を確認する本人確認手段６ｃとを有している。

【００２０】図示された好ましい実施例では、情報端末２は、電話会社の電話管理装置３を介して公衆回線１３，１６で決済管理装置６と接続されている。使用された電話料金及び商品・サービスの提供サイトにおける利用料金は、本人確認後に、金融機関等の決済装置４により決済される。従って、決済管理装置６と決済装置４とは、一般の又は専用の通信回線１７によって接続されている。使用された電話料金及び商品・サービスの提供サイトにおける利用料金は、また、決済管理装置６の代わりに、ダイヤルＱ２と同様に、電話会社により代行徴収するように構成することもできる。この場合、電話管理装置３と決済装置４とは、一般の又は専用の通信回線１４によって接続される。

【００２１】図２０は、図１９に示された本人確認システムによって実行される本発明に係る本人確認方法の一実施形態のフローチャートである。図示されているように、本発明に係る本人確認方法は、商品・サービスの提供サイトに設けられた管理装置に利用者から少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順(ステップ１)と、管理装置から決済サービスセンタに設けられた決済管理装置に、少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順(ステップ２)と、決済管理装置から当該電話番号の情報端末に電話を掛け、少なくとも請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う手順(ステップ３)と、情報端末から決済を行うことを許諾する旨の入力を確認することにより、非現金決済において必要となる本人であることの確認を取る手順(ステップ４)とを含んで構成されている。

【００２２】本発明方法では、日本人であればほとんどの人が所持している携帯可能な情報端末の電話番号を商品・サービスの提供サイトに設けられた管理装置１において利用者から取得し、これを決済管理装置6に通知し、さらに決済管理装置６から当該通知された情報端末２の電話番号を用いて電話を掛け、その情報端末２をその時携帯している者から何らかの行動、具体的には、決済を行うことを許諾する旨の入力か、又は、全く心当たりがないことを理由とする拒否する旨の入力を確認する。管理装置１に情報端末２の電話番号を入力している者がその情報端末２をその時携帯している者でない場合には、全く心当たりがないことを理由とする拒否することとなる。逆に、決済を行うことを許諾する旨の入力があった場合には、管理装置１に情報端末２の電話番号を入力している者がその情報端末２をその時携帯している

者であることを、実質的に証明することとなる。これにより、本人であることの確認が取れることとになり、決済の手続きに移行させることができる。

【００２３】なお、携帯電話の盗難や落し物等により、契約者以外の者の手に携帯可能な情報端末２が渡る可能性も否定できない。このような場合、クレジットカードやデビットカードと同様に、不正拾得者の使用を当該携帯可能な情報端末２の契約者の使用ではないと見破ることはできない。そこで、図示された好ましい実施例では、携帯可能な情報端末そのものには記録されていない各種の個人情報、例えば、携帯可能な情報端末２の電話登録暗証番号、契約者の氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号、指紋など生体データ等、携帯可能な情報端末２の契約者のみが知り得る個人情報のいずれか1つ又は複数を、携帯可能な情報端末２（又は管理装置１）から入力させ、電話会社又は決済管理装置６のメモリに記録されている対応するデータと照合することにより(ステップ５)、本人であることの認証精度を向上させることができる。

【００２４】

【具体例１】図１は、駐車場における本人確認システム及びそれを利用した利用料金決済システムのブロック図である。この利用料金決済システムは、従来、現金や各種のカード、例えば、クレジットカード、デビットカード、プリペイドカード等を用いて支払っていた利用料金を、電話会社が携帯電話の口座から代行徴収するようにしたものである。図示された本人確認システムは、概略的に、駐車場に隣接して設置された管理装置１と、管理装置１に有線、無線各種の通信回線１２を介して接続された決済管理装置６と、駐車場を利用する者が所持する携帯電話等の携帯可能な情報端末２と、情報端末２と決済管理装置６とを通信回線１３、１６を介して接続する電話管理装置３と、そして、電話管理装置３及び決済管理装置６に通信回線１４、１７を介して接続された決済装置４とを含んで構成されている。尚、通信回線１３の少なくとも一部は、情報端末２が携帯可能な情報端末であるため無線通信となる。

【００２５】本システムは、自宅のＰＣを用いた場合等のインターネットを介しての通信販売やＡＳＰ利用の利用料金の支払に伴う認証にも利用することができる。この場合、利用者が用いる情報端末５は、公衆電話回線等の通信回線１５を用いて決済管理装置６に接続され、さらに、インターネット上のバーチャルショップ等には、通信回線１２を介して接続される。また、認証に用いる情報端末２の電話番号も、決済管理装置６を経由して管理装置１に通知される。その後は、駐車場等における管理装置１と同様の手順によって、当該バーチャルショップ等を利用した者が、情報端末２の電話会社と契約した本人であることを認証する。情報端末５は、また、決済管理装置６を経由せずにインターネットを介して直接アクセスするように構成することもできる。

【００２６】駐車場の利用者が所定の情報を管理装置１に入力する際に、管理装置１に設けられたテンキーや画面に表示された数字/文字の部位を押圧することによって行うこともできる。その代わりとして、赤外線等の無線通信により非接触で行うこともできる。車の中から利用者が身を乗り出して入力をする必要がなく、また、雨の日など濡れなくてすむ利点がある。

【００２７】管理装置１は、複数の駐車場に設置される入出場による利用料金を精算する管理装置である。駐車場は、自走ゲート式、コイン式、立体機械式、路上駐車式などである。また、駐車場以外の施設であって入場出場により料金を支払う施設、例えば、レンタカー貸し出し施設などにも設置可能である。また、複数の店舗における買物においても応用可能で、料金を精算するＰＯＳレジに組み込んで設置可能である。店舗は、店員により商品を販売する商店だけでなく、自動販売機など無人の販売機械を含む概念である。前述のように、実販売のほかインターネットなどによる通信販売、インターネットのＡＳＰ利用によるバーチャルショップも含まれる。

【００２８】図２は、図１に示された管理装置１の詳細構成図であり、図３は、駐車場における管理装置１のデータ入力部１０４の一例を示す詳細構成図である。図４は、情報端末２の詳細構成図であり、図５は、電話管理装置３の詳細構成図である。図６は、決済管理装置６の詳細構成図であり、図７は、小売店等の店舗に管理装置1が設置される場合におけるデータ入力部１０４の詳細構成図であり、そして、図８は、情報端末５の詳細構成図である。

【００２９】図２に示されている管理装置１の料金計算・課金部１０１は、入場時間と出場時間から利用料金の計算と売上処理とをし、利用者に対して課金処理をする。後述する店舗使用・通信販売では、買物の集計と売上処理とをし、課金処理をする。表示部１０２は、各種のデータを表示する液晶画面等の画像表示部である。この部位に、数字/文字キーを表示させ、これをテンキーの代わりとして使用することもできる。電話部１０３及び１０９は、電話の送受信、電話番号の通知、暗証番号の記録、電話機器番号など電話機能による照合、認証などを行う。テンキーや表示部１０２に表示された数字/文字エリア等を含むデータ入力部１０４は、利用者が所持している携帯可能な情報端末２の電話番号、認証の精度を向上させるための情報端末２の契約者のみが知り得る個人情報を入力する。

【００３０】認証部１０５は、データ入力部１０４からの各種データと記録部１０６に記録された認証データ、課金データ、決済データ等のデータとを照合し認証する。決済データ部１１１は、予め利用者の住所、氏名、

年令、郵便番号、電話番号、決済口座番号（銀行カード、クレジットカード、デビットカード）など認証の精度向上を図ると共に決済に必要なデータを記録する。時計部１１０は、年月日時間を発生するクオーツ時計等の時計からなる。制御部１０７は、上記各構成要素を用いて本発明に係る本人確認方法を実行するプログラムを制御する。なお、参照番号１０８は、管理装置１を小売店等の店舗に配置した場合における、取扱商品の詳細情報を蓄積する商品データ部である。

【００３１】図３に示されているデータ入力部１０４は、ゲート式駐車場に用いられる管理装置１におけるもので、入場しようとする車を検知する入場検知部１００１と、出場しようとする車を検知する出場検知部１００２と、入場する車の特定のための入力を行う入場テンキー部１００３と、そして、出場しようとする車の特定のための入力を行う出場テンキー部１００４とを備えて構成されている。なお、出場テンキー部１００４は、出場検知部１００２からの検出信号と入場検知部１００１からの検出信号とにより入出を識別できるため、省略することができその場合は入場テンキー部１００３で代用する。

【００３２】図７に示されているデータ入力部１０４は、店舗に設置される管理装置１におけるもので、買物の料金や認証データの基礎となるデータを入力するＰＯＳレジのカードリーダ部２００１とテンキー部２００２とを含んでいる。買物の料金を各種カードで支払う場合に、カード会社の認証方法に加えて本発明の認証により本人であることの確証を得る。例えば、本人であることに多少の疑義がある場合に、本人が所持しているであろう携帯電話に決済管理装置６から電話を掛け、その場で決済管理装置６からの電話を受ける動作により本人確認を行う。利用者は、決済管理装置６からの利用料金の課金対象として、カードとすることも電話料金の支払口座とすることもできる。

【００３３】この場合、カード裏面に設けられた磁気ストリップ、ＩＣカードのメモリなどに情報端末２の電話番号を記録しておくように構成することもできる。買物時に、カードリーダにカードを通してスワイプ操作すると、手動入力より迅速且つ間違いなく情報端末２の電話番号を入手することができる。そして、これを決済管理装置６に通知することができる。また、カード内に予め認証データを入れておくことで、決済管理装置６は電話会社に認証データを照会しなくても情報端末２からの認証データと照合・認証することもできる。また、上記テンキーの代わりに赤外線送受信機等の非接触入力装置を用いることもできる。

【００３４】図４に図示された情報端末２は、利用者が携帯する携帯電話、ＰＤＡなどの情報電話端末であって、決済諾否入力部２０１と、表示部２０２と、電話の受発信機能を有する電話部２０３と、データ入力部２０４と、認証部２０５と、記録部２０６と、そして、制御部２０７とを含んで構成される。各部における基本的機能は、前述した管理装置１における対応する構成要素のそれと同様であるので、詳細な説明は省略する。また、情報端末２と管理装置１とに、それぞれ赤外線受発信素子を別途に設けることで、非接触で情報端末２のデータ入力部２０４から入力した各種のデータを管理装置１へ入力することができる。また、指紋入力部を別途設けることで認証することができる。

【００３５】図８に図示された情報端末５は、通信販売利用時やインターネットのＡＳＰ利用時に、利用者が用いるものである。駐車場や小売店等の店舗における本人確認方法では、利用者が商品・サービスの提供サイトに設けられた管理装置１の場所で認証データの入力を行う。それに対して、本実施例のような通信販売利用やインターネットのＡＳＰ利用では、利用者は遠隔地からインターネット等の通信回線を介して管理装置１に接続される。利用者端末５は、携帯可能な、または、卓上の携帯電話、ＰＤＡ、パソコンなどの情報通信端末であって、決済諾否入力部５０１と、表示部５０２と、電話の受発信機能を有する電話部５０３と、データ入力部５０４と、認証部５０５と、記録部５０６と、そして、制御部５０７とを含んで構成される。各部における基本的機能は、前述した管理装置１における対応する構成要素のそれと同様であるので、詳細な説明は省略する。

【００３６】図５に図示された電話管理装置３は、ＮＴＴドコモ社等の携帯電話会社に設置されるもので、電話番号によって特定される外部の情報端末２に回線を接続する電話部３０１、３０２、３０７と、認証データや決済データを予め登録しておく決済データ部３０４と、情報端末２の機器識別データやサービス・物販識別データなどの認証を行う認証部３０５と、そして、駐車場や店舗などでの利用料金や通話料金は受信先課金機能などにより課金するが、これらデータを記録する記録部３０６とを備えて構成されている。

【００３７】図６に示された決済管理装置６は、決済サービスセンタに設けられるもので、電話番号によって特定される外部の端末、例えば、電話管理装置３や決済装置４に回線を接続する電話部６０１、６０２、６０７と、電話料金、課金データの内の利用料金及び決済データを決済装置４に送信し決済する等の制御を行う制御部６０３と、認証データや決済データを予め登録しておく決済データ部６０４と、電話管理装置３からの認証データ、課金データ及び決済データと管理装置１からの認証データ、課金データ及び決済データとを照合し認証する認証部６０５と、電話料金、課金データの内の利用料金及び決済データを記録する記録部６０６とを含んで構成されている。図示された好ましい実施例では、さらに、地図情報を記録した地図データ部６０８も有している。無人管理の場合に、管理装置１の場所と関連づけするこ

とにより、複数の管理装置１の利用状況を固定または携帯可能な情報端末（図示せず）で把握管理することができる。

【００３８】金融機関の決済装置４は、電話管理装置３からの電話料金と課金データの内の利用料金などを、利用者口座から電話会社口座へ、また、電話会社口座から駐車場、店舗口座へ振替え決済をする。通信回線１２，１３，１４，１５，１６，１７は、必用に応じて、ＩＳＤＮ回線、インターネット回線、ＰＨＳ回線などの種々の回線手段を用いることができる。認証データは、予め電話会社の電話管理装置３と、決済サービスセンタの決済管理装置６と、駐車場・店舗の管理装置１（店舗のＰＯＳレジ）に使用されるカード内の１つ以上に記録することができる。

【００３９】この認証データとしては、情報端末２の電話番号の他、（１）自由な暗証番号、管理装置１が自動的に発行するランダムな暗証番号、電話利用以外のソフト情報・物販などで利用する利用者識別番号であるサービス・物販利用者識別データ、発信者番号通知による電話番号、電話機器識別データである電話機器番号、管理装置１の電話番号、管理装置１の装置識別データである装置番号、情報端末２から入力する諾否データや管理装置１の自動発行にかかる決済番号である決済の諾否データ、及び、（２）情報端末２の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号と、決済データの暗証番号、指紋など生体データなど情報端末２の契約者のみが知っている個人情報である。前者は、携帯端末である情報端末２とシステムの各装置との間の相互の認証に、後者は利用者本人であることの確認の精度向上のためのデータとして使用する。

【００４０】課金データは、年月日日時、データ管理番号、駐車場名、入出場時間、店舗名、通販管理番号、商品名、数量、利用料金（金額）などからなる。受信者課金データは、受信者に課金するデータの識別番号である。サービス・物販識別データは、電話利用以外のソフト情報・物販などの識別番号である。決済データは、予め利用者が登録する銀行の決済口座番号、クレジットカード番号などで、氏名、年令、住所、郵便番号、電話番号、暗証番号など個人を特定するデータとリンクし、決済を可能とするデータである。入場の有無データは、駐車場の利用の有無を管理装置１のデータ入力部１０４より入力する有り：１、無し：０と自動発行される決済番号である。

【００４１】次に、図９～図１１を用いて、ゲート式駐車場を利用する場合における本発明に係る本人確認方法及び認証後における決済の流れを説明する。図９は、ゲート式駐車場に車を入場する時の流れを示すフローチャートである。図１０は、ゲート式駐車場から車を出場する時の流れを示すフローチャートである。図１１は、ゲート式及びコイン式駐車場を利用した場合のデータ表の一例である。図９に示されているように、ゲート式駐車場に入場しようとすると、管理装置１の入場検知部１００１（図３参照）が車の進入を検知する(ステップ１１)。この時、利用者は、入場テンキー部１００３から利用者の認証データのうち、少なくとも情報端末２の電話番号と自由な暗証番号を入力する(ステップ１２)。高いセキュリティを求めるときは、情報端末の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末２の契約者のみが知り得る個人情報も同時に入力する。

【００４２】管理装置１の認証部１０５に、上記電話番号を照会し、入場がないことをチェックした後、管理装置１の記録部１０６に認証データのうち少なくとも情報端末２の電話番号と自由な暗証番号と入場時刻を記録する(ステップ１３)。次に、電話部１０３から決済管理装置６の第１電話部６０１（図６参照）に電話し、データに入場有りデータを追加し、送信する(ステップ１４)。決済管理装置６は、データにサービス・物販識別データ（例えば、駐車場料金を示す＃０８８０などの文字列）と、受信者課金データ（例えば、ＸＸＸ氏への課金を行うためのデータである＃１０８などの文字列）とを追加し、記録部６０６に記録する。一方、第２電話部６０２から電話管理装置３の第１電話部３０１に電話し、前記データを送信する(ステップ１５)。

【００４３】電話管理装置３では、決済データ部３０４に記録された認証・決済データと、前記データのサービス・物販識別データと、そして、受信者課金データとを認証部３０５で認識し、記録部３０６に記録する。並行して、情報端末２に前記データの内、サービス・物販識別データ以外のデータを送信する(ステップ１６)。利用者は、情報端末２から認証データのうち少なくとも自由な暗証番号と入場の有データ〝入場する：１〟を入力し、管理装置１に返信する(ステップ１７)。管理装置１の認証部１０５が認証データのうち少なくとも自由な暗証番号と入場の有データである〝入場する：１〟を認識した場合、それを記録部１０６に記録する。これにより、入場検知部１００１のゲートが開き入場できる状態となる(ステップ１８)。

【００４４】また、入場の無データである〝入場しない：０〟の返信の場合は、入場できない状態が継続する。入場データは、また、決済サービスセンタの決済管理装置６に送信し、記録部６０６に記録する。決済管理装置６は、これら入場データから地図情報記録の手段及び管理装置１の場所と関連づけする手段を持つ地図データ部６０８で、複数の管理装置１の利用状況を把握することができる。また、第３電話部６０７から、このよう

な利用状況データを固定または携帯可能な情報端末に送信することができる。（図示なし）

【００４５】一方、ゲート式駐車場から出場するときには、図１０に示されているように、出場検知部１００２で車を検知する(ステップ２１)。この時、利用者は、出場テンキー部１００４から、利用者の認証データのうち少なくとも情報端末２の電話番号と自由な暗証番号を入力する(ステップ２２)。高いセキュリティを求めるときは、入場時に入力した個人情報、例えば、情報端末の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末の契約者のみが知り得る個人情報も同時に入力する。駐車場の入場と出場において、管理装置１での照合・認証は、図１１に図示したように、電話番号、駐車場名、入場ゲート関連番号と出場ゲート関連番号によって照合し、認証することによって短時間に照合・認証作業を完了することができる。

【００４６】このように、管理装置１の認証部１０５で、認証データのうち少なくとも情報端末２の電話番号を照合、認証する(ステップ２３)。記録部１０６には、電話番号及び自由な暗証番号と出場時刻を記録する。一方、入場時刻と出場時刻から利用料金を料金計算・課金部１０１で計算し、認証データのうち少なくとも情報端末２の電話番号及び自由な暗証番号から課金すべき口座を特定して課金し、並行して、課金データとして記録部１０６に記録する(ステップ２４)。

【００４７】管理装置１は、上記認証データである情報端末２の電話番号と自由な暗証番号とに課金データを追加し、決済サービスセンターの決済管理装置６に、これらを送信する(ステップ２５)。決済管理装置６は、上記認証データである情報端末２の電話番号と、課金データに、（さらに、サービス・物販識別データ（例えば＃０８８０などの文字列）と、受信者課金データ（例えば＃１０８などの文字列）と、発信者番号通知設定案内と、サービス・物販利用者識別データ入力案内と、決済データの暗証番号入力案内等を追加しても良い。）自由な暗証番号入力案内と、決済の諾否問合せデータとを追加し、電話会社の電話管理装置３を経由し情報端末２に送信する(ステップ２６)。並行して、これらのデータは、決済管理装置６の記録部６０６に記録される。

【００４８】前記（ ）内の追加データの場合、電話管理装置３の認証部３０５で、サービス・物販識別データと受信者課金データを認証し、課金すべき受信者毎に課金データ及び決済の諾否データを記録部３０６に記録し、並行して情報端末２に送信する(ステップ２７)。利用者は、認証データである情報端末２の電話番号と課金データを確認する。（さらに、サービス・物販識別データの確認と、受信者課金データと、発信者番号通知設定と、サービス・物販利用者識別データと、決済データの暗証番号などを追加しても良い。）自由な暗証番号と、決済諾否データである"決済する：１"を入力し、電話管理装置３を経由し、決済管理装置６に送信する(ステップ２８)。決済管理装置６は、上記認証データを照合・認証し、記録する。合格すると、認証データである、情報端末２の電話番号と、課金データと、（さらに、受信者課金データと、発信者番号通知の電話番号と、サービス・物販識別データと、サービス・物販利用者識別データと、決済データの暗証番号等を追加しても良い。）決済許諾データである"決済する：１"を、それぞれ、電話管理装置３と管理装置１に送信し、記録する。

【００４９】管理装置１の出場検知部１００１はゲートを開き、車両が出場できる状態とする(ステップ２９)。また、決済の拒否データである"決済しない：０"の返信の場合は、出場できない。決済に際して決済管理装置６は、図１２に示すように、認証データである情報端末２の電話番号と、課金データと、（さらに、電話機器識別データと、発信者番号通知の電話番号と、サービス・物販識別データ（例えば＃０８８０などの文字列）と、受信者課金データ（例えば＃１０８などの文字列）と、サービス・物販利用者識別データと、決済データの暗証番号などを追加しても良い。）を電話管理装置３に送信する(ステップ３１)。

【００５０】電話管理装置３は、認証部３０５に予め登録されている認証データと照合・認証する(ステップ３２)。合格すると、認証データを決済管理装置６と、管理装置１と、そして、情報端末２に送信する。

（１）電話管理装置３の料金の回収を決済管理装置６が代行する本実施例では、電話管理装置３から決済管理装置６を経由し、決済装置４へ利用者の決済口座番号と、課金データを送信し(ステップ３７)、決済装置４で利用者の口座振替を行うことも可能である。決済装置４は、個々の携帯可能な情報端末利用者の口座から決済管理装置６の口座へ商品・サービス利用料金の振替を行う(ステップ３８)。さらに、決済管理装置６の口座から商品・サービスの提供者である駐車場・店舗の銀行口座へ振替決済する(ステップ３９)。この場合、電話料金は、電話管理装置３から決済装置４へ直接送信し、商品・サービスの利用料金とは別扱いになる。

【００５１】また、料金の回収を決済管理装置６が行う場合に、予め認証データを決済管理装置６に登録して、これを用いて認証し、利用者の決済口座番号及び課金データを決済装置４へ送信し決済することも可能である。

（２）一方、料金の回収を電話管理装置３が行う実施例では、電話管理装置３から金融機関の決済装置４へ情報端末２の電話番号の決済口座番号と、電話料金と、課金データを送信する(ステップ３３)。決済装置４は、利用者の口座から電話会社の口座へ商品・サービス利用料金及び電話料金の振替を行う(ステップ３４)。さらに、電話会社口座から、駐車場・店舗の銀行口座へ振替決済す

る(ステップ３５)。

【００５２】また、この場合に、氏名、郵便番号、年令、住所の一部、電子メールアドレス、支払先金融機関名、口座番号などを情報端末２から入力させ、認証することで一層の機器認証と本人確認のセキュリティを高めることができる。また、決済サービスセンターの決済管理装置６は、これら出場データから、地図情報記録手段及び管理装置１の場所と関連づけする手段を持つ地図データ部６０８で、複数の管理装置１の利用状況を把握することができる。また、第３電話部６０７から固定または携帯可能な情報端末に利用状況データを送信することができる。

【００５３】また、管理装置１が自動的に発行するランダムな暗証番号を情報端末２に表示し、利用者が管理装置１から入力するランダムな暗証番号を管理装置１で照合・認証することも可能である。以上、ゲート式駐車場について詳細に説明したが、駐車時及び駐車終了時にそれぞれ図９及び図１０に示された入場時及び出場時における操作を行うことにより、路上駐車式の駐車スペースに対しても応用可能である。また、この路上駐車場などで、入場時に最低利用料金を先に課金し、徴収することも可能で、さらに、追加利用料金を携帯電話から継続利用料金を行う課金データを送信することで継続使用が可能となる。また、ここに示した駐車場利用、店舗での買物、通信販売、インターネットのＡＳＰ 利用以外にもレンタル利用、ガソリンスタンド利用にも利用できる。

【００５４】

【実施例２】次に、車両が駐車スペースに駐車した場合に、車両下方に設けられたフラップが所定高さまで持ち上がり車両の出場を許さないように構成したフラップ式駐車場利用の例について説明する。図１３は、フラップ式駐車場に入場するときの流れを示すフローチャートであり、図１４は、フラップ式駐車場から出場するときの流れを示すフローチャートである。フラップ式駐車場においては、入場時、入場検知部１００１が車を検知する(ステップ４１)と自動的に駐車スペースの番号に対応するフラップ番号と入場時刻が管理装置１の記録部１０６に記録される(ステップ４２)。車両が当該駐車スペースに駐車してから所定時間後、入場検知部１００１はフラップを所定高さまで持ち上げ車両が駐車スペースから出られないようにする(ステップ４３)。なお、このため、ゲート式駐車場の入場時のように認証行為は行なわない（図９参照）。次に、出場部１００２は、車両の駐車を検知し続けている(ステップ５１)。出場に際して、駐車場利用者は、出場テンキー部１００４からフラップの番号と、利用者の認証データのうち少なくとも情報端末２の電話番号と、そして、自由な暗証番号を入力する。管理装置１の記録部１０６にフラップ番号と上記電話番号と自由な暗証番号と出場時刻を記録する(ステップ５２)。管理装置１の記憶部１０６に、フラップ番号と、利用者が所有している情報端末２の電話番号と、自由な暗証番号、そして、出場時刻を記憶する(ステップ５３)。

【００５５】管理装置１の料金計算・課金部１０１は、入場時刻と出場時刻から利用料金を計算し、課金処理を行う(ステップ５４)。次に、電話部１０３から決済管理装置６に電話をし、認証データと、そして、課金データとを送信する(ステップ５５)。決済管理装置６は、認証データである情報端末２の電話番号と、課金データに、（さらに、サービス・物販識別データ（例えば＃０８８０などの文字列）と、受信者課金データ（例えば＃１０８などの文字列）と、発信者番号通知設定案内と、サービス・物販利用者識別データ入力案内と、決済データの暗証番号入力案内などを追加しても良い。）自由な暗証番号入力案内と、決済の諾否問合せデータとを追加し、電話会社の電話管理装置３に送信する(ステップ５６)。

【００５６】電話管理装置３は、サービス・物販識別データと受信者課金データとを認証し、課金データと決済の諾否問合せデータを情報端末２に送信する(ステップ５７)。前記(　)内の追加データの場合も、電話管理装置３で、サービス・物販識別データと受信者課金データを認証し、課金データと決済の諾否データを情報端末２に送信する。利用者は、情報端末２から認証データである情報端末２の電話番号と課金データ（さらに、サービス・物販識別データと、受信者課金データと、発信者番号通知設定と、サービス・物販利用者識別データと、決済データの暗証番号等を追加しても良い。）を確認する。自由な暗証番号と、決済諾否データである"決済する：１"を入力し、電話管理装置３を経由し決済管理装置６に送信する(ステップ５８)。

【００５７】決済管理装置６は、上記認証データを照合・認証し、記録する(ステップ５９)。合格すると、認証データである情報端末２の電話番号と、課金データと、（さらに、受信者課金データと、発信者番号通知の電話番号と、サービス・物販識別データと、サービス・物販利用者識別データと、決済データの暗証番号などを追加しても良い。）、決済許諾データである"決済する：１"を、電話管理装置３と管理装置１に送信する(ステップ６０)。出場検知部１００１のフラップが下がり(ステップ６１)、車両は出場できる。また、決済の拒否データである"決済しない：０"の返信の場合は、出場できない。また、決済の方法や高いセキュリティの設定は、ゲート式駐車場利用の例と同様に行うことができる。また、機械式立体駐車場も同様な処理となる。

【００５８】

【実施例３】次に、小売店等の店舗において買い物をする際に、その利用者が所持する携帯可能な情報端末２の電話会社による高信用力の認証を利用することにより、利用料金の課金及び決済する方法とシステムの例について説明する。図１５は、店舗で買い物利用したときの流

れを示すフローチャートであり、図１６は、店舗での買い物利用のデータ表例を示す図である。システムの詳細は、基本的に図１に示されたものと同様であるためその説明は省略する。

【００５９】店舗で買い物利用したときの流れは、まず、店舗の管理装置１の料金計算・課金部１０１で買物料金の集計をし、課金処理をする。並行して、これを記録部１０６に記録する(ステップ７１)。次に、図７に示されたデータ入力部１０４のカードリーダ部２００１やテンキー部２００２を用いて、利用者の認証データのうち少なくとも情報端末２の電話番号と自由な暗証番号を入力をする(ステップ７２)。なお、カードに利用者の電話番号を記録しておき、買物時、カードリーダ部２００１により当該記録を読み込むと手動入力より処理が早く且つ間違いないようにすることができる。

【００６０】また、高いセキュリティを求めるときは、情報端末２の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末の契約者のみが知り得る個人情報も同時に入力する。一方、管理装置１の記録部１０６は、データ管理番号（ＰＯＳ機器番号と売上連番）と、上記電話番号と、自由な暗証番号と、売上時刻を記録する(ステップ７３)。管理装置１は、上記認証データである情報端末２の電話番号と自由な暗証番号に、課金データを追加し、決済サービスセンタの決済管理装置６にこれらを送信する(ステップ７４)。

【００６１】決済管理装置６は、上記認証データである情報端末２の電話番号と課金データに（さらに、サービス・物販識別データ（例えば＃０８８０などの文字列）と、受信者課金データ（例えば＃１０８などの文字列）と、発信者番号通知設定案内と、サービス・物販利用者識別データ入力案内と、決済データの暗証番号入力案内などを追加しても良い。）、自由な暗証番号入力案内と、決済の諾否問合せデータとを追加し、電話会社の電話管理装置３を経由し情報端末２に送信する(ステップ７５)。

【００６２】前記(　)内の追加データの場合も、電話管理装置３で、サービス・物販識別データと受信者課金データを認証し、課金データと決済の諾否データを情報端末２に送信する。利用者は、携帯可能な情報端末２で、認証データである情報端末２の電話番号と、課金データを確認する。（さらに、サービス・物販識別データの確認と、受信者課金データと、発信者番号通知設定と、サービス・物販利用者識別データと、決済データの暗証番号等を追加しても良い。）しかる後、自由な暗証番号と、決済諾否データである"決済する：１"を入力し、電話管理装置３を経由し決済管理装置６に送信する(ステップ７６)。

【００６３】決済管理装置６は、上記認証データを照合・認証し、記録する(ステップ７７)。合格すると、認証データである情報端末２の電話番号と、課金データと、（さらに、受信者課金データと、発信者番号通知の電話番号と、サービス・物販識別データと、サービス・物販利用者識別データと、決済データの暗証番号などを追加しても良い。）決済許諾データである"決済する：１"を電話管理装置３と管理装置１に送信する(ステップ７８)。情報端末２から認証データのうち少なくとも自由な暗証番号と決済の許諾データである" 決済する：１"が管理装置１に返信されると、管理装置１の認証部１０５で認証データのうち少なくとも自由な暗証番号と決済の許諾データである"決済する：１"を認証し、記録部１０６に記録し、売上処理を終了する(ステップ７９)。決済管理装置６は、さらに、電話管理装置３に課金データを送信する(ステップ８０)。また、決済の拒否データである"決済しない：０"の返信の場合は、売上処理することなくキャンセルする。また、決済の方法や高いセキュリティの設定は、前述したゲート式駐車場利用の例による。

【００６４】

【実施例４】次に、通信販売、インターネットのＡＳＰ利用の際に、その利用者が所持する携帯可能な情報端末２の電話会社による高信用力の認証を利用することにより、利用料金の課金及び決済する方法とシステムの例について説明する。図１７は、通信販売利用したときの流れを示すフローチャートであり、図１６は、通信販売利用におけるデータ表例を示す図である。本態様におけるシステムは、基本的に、図１に示されたものに、通信回線１５を介して決済管理装置６に接続された携帯可能な又は固定式の利用者端末５を追加したものである。

【００６５】まず、利用者は、情報端末５のデータ入力部５０４から店舗の管理装置１の電話部１０９に電話接続する(ステップ９１)。情報端末５のデータ入力部５０４を用いて商品データ部１０８に記録されていた商品の選択し、料金計算・課金部１０１で料金を計算、課金処理し、これらを通販管理番号とともに記録部１０６に記録する(ステップ９２)。利用者は、さらに、利用者の認証データのうち少なくとも情報端末２の電話番号と自由な暗証番号を入力する。これらデータは、売上時刻とともに記録部５０６、１０６に記録される(ステップ９３)。

【００６６】管理装置１の電話部１０３は、決済管理装置６に電話をし、サービス・物販識別データと、受信者課金データと、そして、課金データとを送信する(ステップ９４)。決済管理装置６は、上記認証データである情報端末２の電話番号と、課金データに、（さらに、サービス・物販識別データ（例えば＃０８８０などの文字列）と、受信者課金データ（例えば＃１０８などの文字列）と、発信者番号通知設定案内と、サービス・物販利

用者識別データ入力案内と、決済データの暗証番号入力案内等を追加しても良い。）自由な暗証番号入力案内と、決済の諾否問合せデータとを追加し、電話会社の電話管理装置３を経由し、情報端末２に送信する(ステップ９５)。

【００６７】前記(　)内の追加データの場合も、電話管理装置３でサービス・物販識別データと、受信者課金データを認証し、課金データと、決済の諾否問合せデータを情報端末２に送信する。電話管理装置３では、サービス・物販識別データと、受信者課金データを認証し、課金データと決済の諾否問合せデータを携帯可能な情報端末２に送信する(ステップ９６)。利用者は、情報端末２で、認証データである情報端末２の電話番号と課金データを確認する。（さらに、サービス・物販識別データの確認と、受信者課金データと、発信者番号通知設定と、サービス・物販利用者識別データと、決済データの暗証番号などを追加しても良い。）自由な暗証番号と決済諾否データである"決済する：１"を入力し、電話管理装置３を経由し、決済管理装置６に返送する(ステップ９７)。

【００６８】決済管理装置６は、上記認証データを照合・認証し、記録する(ステップ９８)。合格すると、認証データである情報端末２の電話番号と、課金データと、（さらに、受信者課金データと、発信者番号通知の電話番号と、サービス・物販識別データと、サービス・物販利用者識別データと、決済データの暗証番号などを追加しても良い。）決済許諾データである"決済する：１"を電話管理装置３と管理装置１に送信する(ステップ９９)。決済管理装置６から認証データのうち少なくとも自由な暗証番号と決済の許諾データである" 決済する：１"が管理装置１に返信されると、管理装置１の認証部１０５で認証データのうち少なくとも自由な暗証番号と決済の許諾データである"決済する：１"を認証し、記録部１０６に記録し、売上処理を終了する(ステップ１００)。また、決済の拒否データである"決済しない：０"の返信の場合は、売上処理をせず、キャンセルする。また、決済の方法や高いセキュリティの設定は、ゲート式駐車場利用の例による。

【００６９】

【発明の効果】請求項１に記載の本発明は、商品・サービスの提供サイトに設けられた管理装置に少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順と、管理装置から決済サービスセンタに設けられた決済管理装置に、少なくとも利用者の所持する携帯可能な情報端末の電話番号を通知する手順と、決済管理装置から当該電話番号の情報端末に電話を掛け、少なくとも請求原因とその金額を提示して決済を行うことを許諾するか否かの問合せを行う手順と、情報端末から決済を行うことを許諾する旨の入力を確認することにより、非現金決済において必要となる本人認証手順とを含んで構成されてなるため、多くの日本人が所持している携帯可能な情報端末の電話会社による信用力の有る認証を各種の非現金決済において必要となる本人であることの認証に利用した本人確認方法を提供することができる効果を有する。

【００７０】請求項２に記載の本発明は、本人確認を取る手順において、携帯可能な情報端末の電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号、クレジットカード番号、デビットカード番号、決済データの暗証番号等、携帯可能な情報端末の契約者のみが知り得る個人情報のいずれか1つ又は複数とを組み合わせるため、簡単な手順の付加で認証の精度を飛躍的に向上させることができる本人確認方法を提供することができる効果を有する。

【００７１】請求項３に記載の本発明は、利用者から管理装置への通知手順において、利用者が管理装置に設けられた入力装置を用いて直接入力する、利用者が所持している携帯可能な情報端末から無線通信により非接触入力する、又は、利用者が有するインターネット等の通信回線に接続可能な第二情報端末から電話回線などの通信回線を介して入力するため、適宜の手法で携帯可能な情報端末の電話番号を管理装置に通知することができる本人確認方法を提供することができる効果を有する。請求項４に記載の本発明は、本人確認を取る手順において、利用者が管理装置から入力する自由な暗証番号と、利用者が所持している携帯可能な情報端末から入力する自由な暗証番号を、決済管理装置で照合・認証することから簡単な構成により認証の精度を向上させることができる本人確認方法を提供することができる効果を有する。

【００７２】請求項５に記載の本発明は、本人確認を取る手順において、管理装置が自動的に発行するランダムな暗証番号を携帯可能な情報端末にて提示し、利用者が管理装置から入力するランダムな暗証番号を、決済管理装置で照合・認証することから簡単な構成により認証の精度を向上させることができる他の本人確認方法を提供することができる効果を有する。通常行われている駐車場、店舗の管理装置への電話番号や課金データは、複数の数字や文字を順番に入力し、一遍には入力できない事項である。本発明では、利用者が入力する携帯電話番号は本人が良く知っている事項であり、決済の諾否データも「１」または「０」を入力するだけで足りる利点を有している。また、利用者が入力する電話番号のほか自由な暗証番号、電話登録暗証番号、氏名、郵便番号、年令、住所の一部、電子メールアドレス、支払先金融機関名、口座番号などは本人が良く知っている事項である。従って、本発明では、データ入力が容易で、正確に且つ迅速に処理することができる。

【００７３】電話機能を利用することで電話会社の信用力の有る認証機能を利用することができる。また、電話番号を認証データとし電話利用機器の認証と利用者が特

定できる利点を有する。また、電話利用機器と関係する電話登録暗証番号、氏名、郵便番号、年令、住所、電子メールアドレス、支払先金融機関名、口座番号などの認証データで本人を特定し、また、利用するその場で自由な暗証番号を入力することで本人しか分からない一回限りのＩＤ番号の認証データを設定することが可能となる利点を有する。従って、これらの認証データを利用者本人が入力し、利用側と支払側の機器を認証することで高度な安全性が保てる。

【００７４】また、管理装置１と情報端末２との通信および情報端末２の無線通信により非接触で認証データを入力することで管理装置１、情報端末５などの設置場所から入力していることの特定ができ一層の安全性が保てる。さらにまた、情報端末２で指紋などの生体データを入力し、認証することでも一層の安全性が保てることになる。また、営業などのビジネスにおけるＰＣやＰＤＡなどの携帯端末からのデータサーバへのアクセスの認証に、現在、持っている携帯電話などを利用して認証でき、容易にシステムを構築できる利点を有している。

【図面の簡単な説明】

【図1】駐車場における本人確認システム及びそれを利用した利用料金決済システムのブロック図である。

【図２】図１に示された管理装置１の詳細構成図である。

【図３】駐車場における管理装置１のデータ入力部１０４の一例を示す詳細構成図である。

【図４】情報端末２の詳細構成図である。

【図５】電話管理装置３の詳細構成図である。

【図６】決済管理装置６の詳細構成図である。

【図７】小売店等の店舗に管理装置1が設置される場合におけるデータ入力部１０４の詳細構成図である。

【図８】情報端末５の詳細構成図である。

【図９】ゲート式駐車場に車を入場する時の流れを示すフローチャートである。

【図１０】ゲート式駐車場から車を出庫する時の流れを示すフローチャートである。

【図１１】ゲート式及びコイン式駐車場を利用した場合のデータ表の一例である。

【図１２】決済管理装置６における決済の流れを示すフローチャートである。

【図１３】フラップ式駐車場に入場するときの流れを示すフローチャートである。

【図１４】フラップ式駐車場から出場するときの流れを示すフローチャートである。

【図１５】店舗で買い物利用したときの流れを示すフローチャートである。

【図１６】店舗での買い物利用のデータ表例を示す図である。

【図１７】通信販売利用したときの流れを示すフローチャートである。

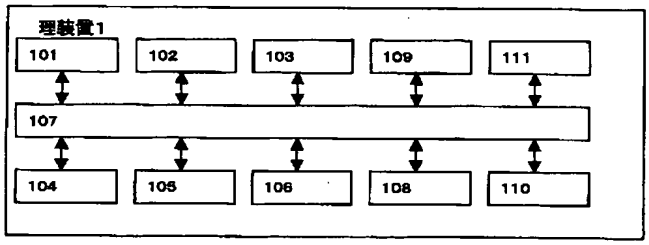
【図１８】通信販売利用におけるデータ表例を示す図である。

【図１９】本発明に係る本人確認システムの一実施形態のブロック図である。

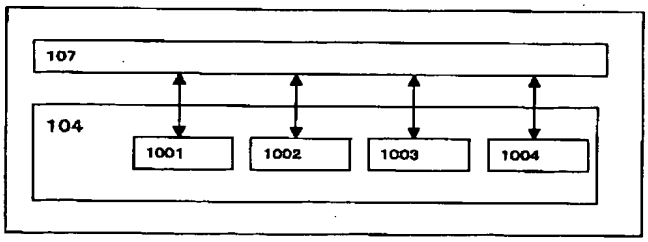
【図２０】図１９に示された本人確認システムによって実行される本発明に係る本人確認方法の一実施形態のフローチャートである。

１　管理装置
２　情報端末
３　電話管理装置
４　決済装置
５　情報端末
６　決済管理装置
１２～１７　通信回線

【図２】



【図３】

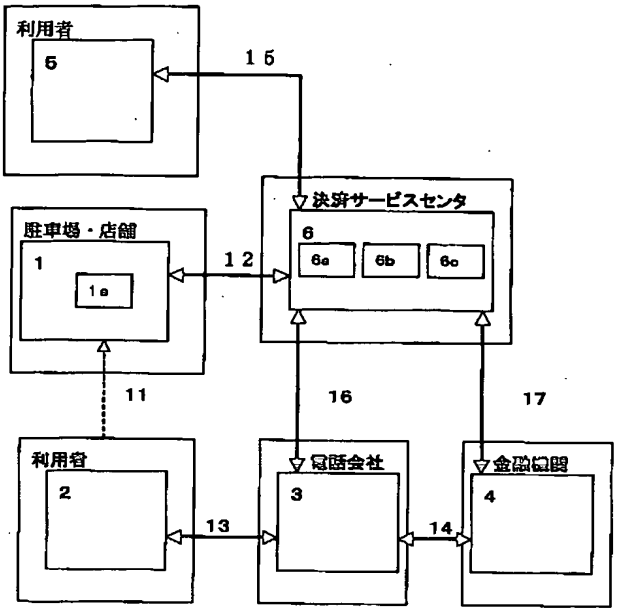


【図１１】

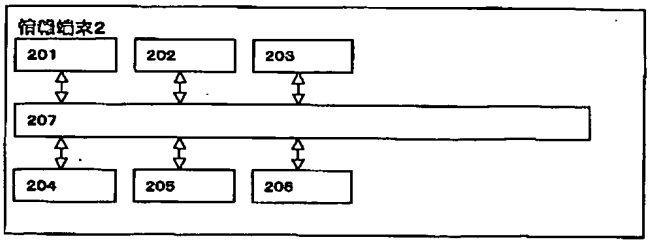
＊１	駐車場名	ｹﾞｰﾄ識別番号	入場時刻	出場時刻	フラップ番号	入場有無	電話番	＊２	利用料金(円)
＃０８８０	AABB	入01/出02/出03	10:10 2000.07.01	12:15 2000.07.01	———	1	09012347788	＃１０８	900

＊１：サービス・　販識別データ
＊２：受信者課金データ

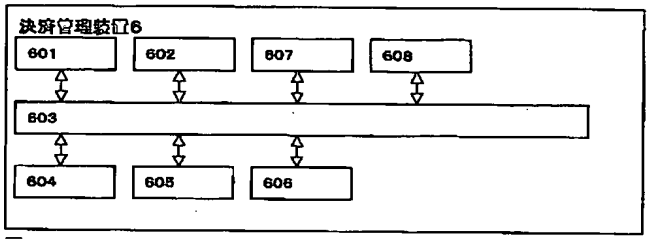
【図１】



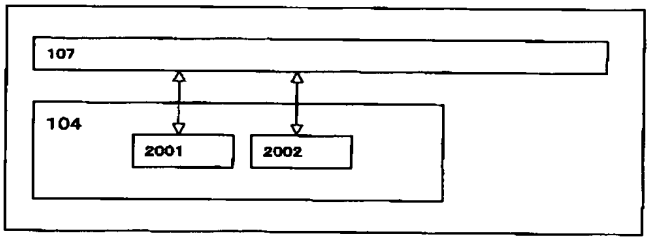
【図４】



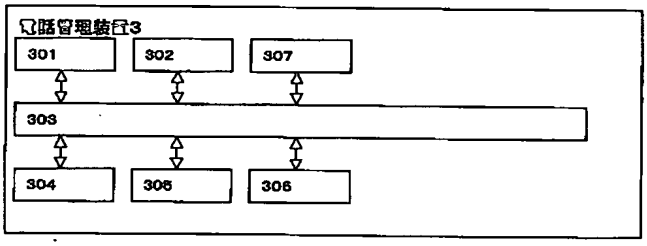
【図６】



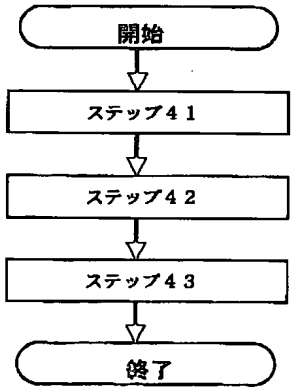
【図７】



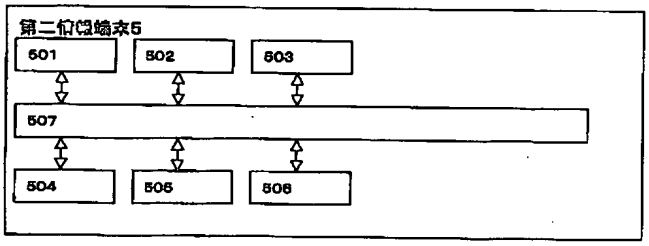
【図５】



【図１３】



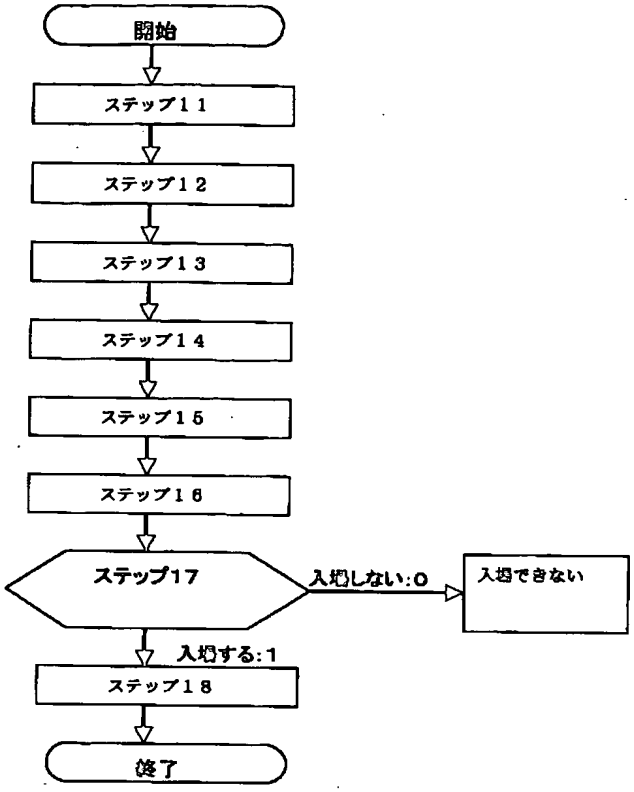
【図８】



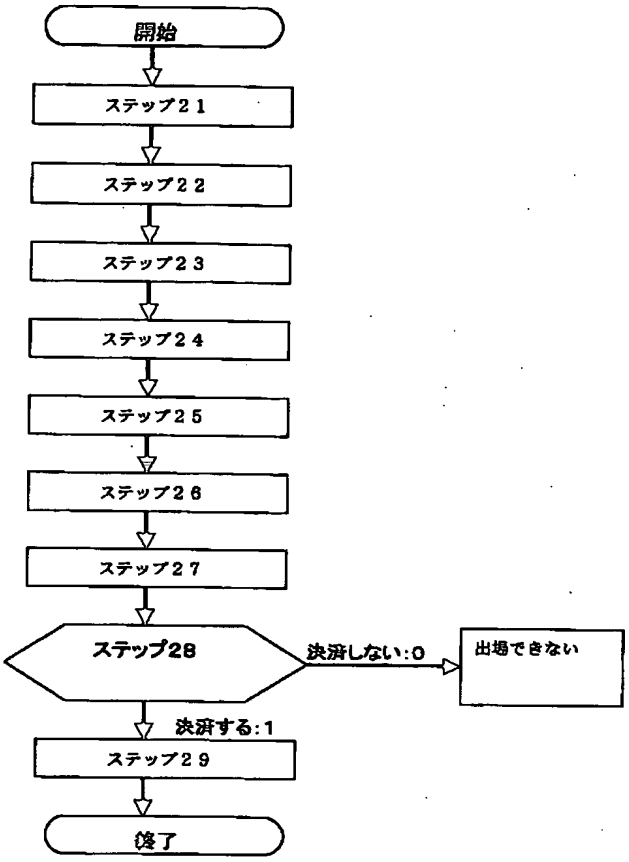
【図１６】

年月日	売上時間	電話番号	認証データ	店舗名	データ管理番号	商品番号	商品名	個数	売上金額(円)
2000.07.01	11:20	03012347788	452	AAAA	007878	A1357	BBBB	2	10,000

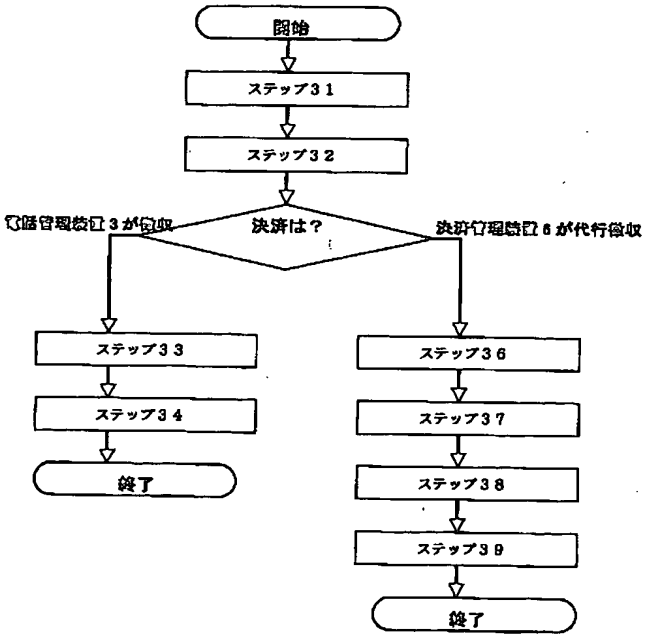
【図９】



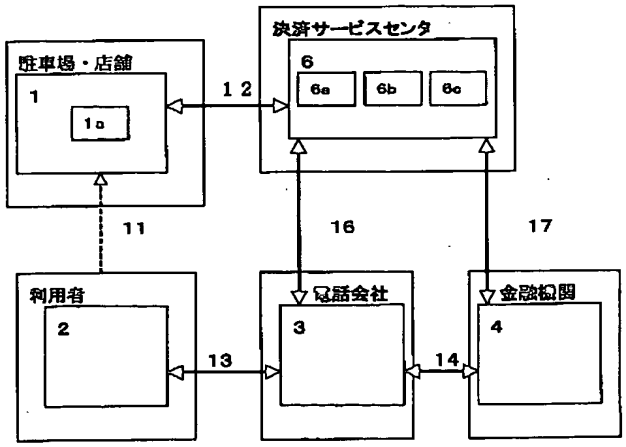
【図１０】



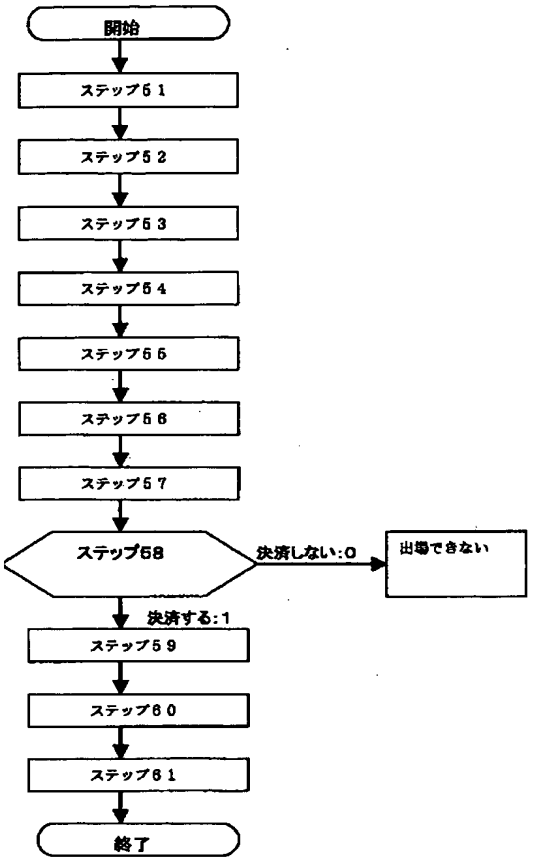
【図１２】



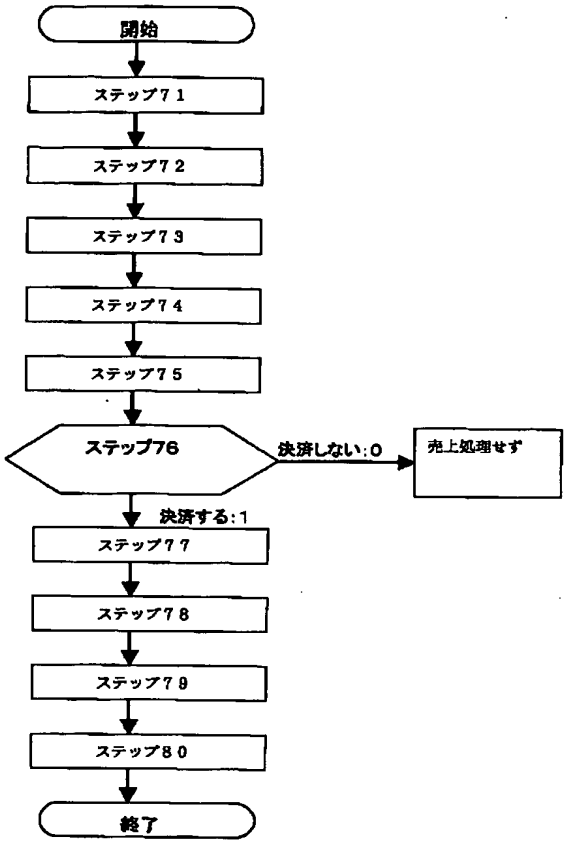
【図１９】



【図１４】



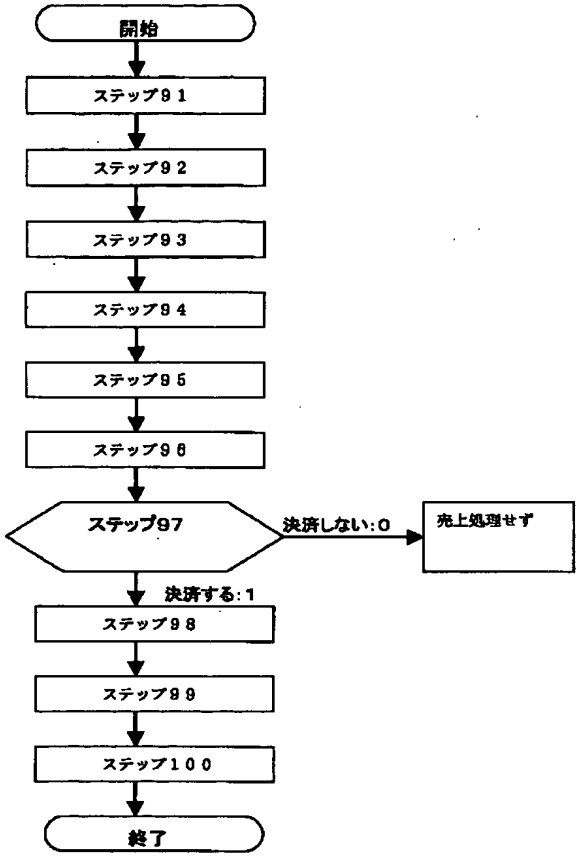
【図１５】



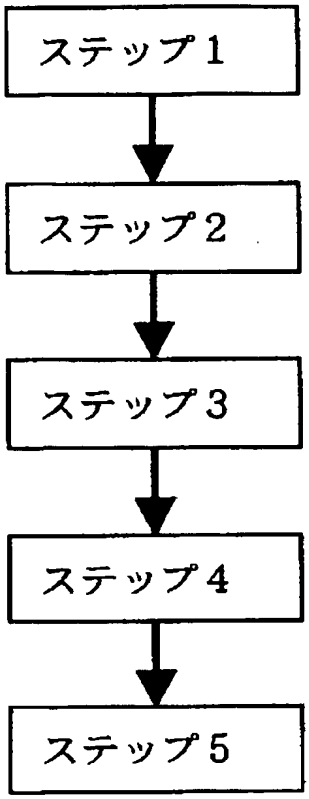
【図１８】

年月日	売上時刻	電話番号	認証データ	通販店舗名	通販管理番号	商品番号	商品名	数量	売上料金(円)
2000.07.01	11:30	09012347788	452	AAAA	010010	A1357	BBBB	3	6,000

【図１７】



【図２０】



フロントページの続き

(72)発明者　荻田　健之
愛知県名古屋市名東区亀の井１－133住友高針荘Ａ棟104号
(72)発明者　磯部　俊哉
東京都渋谷区道玄坂１－21－２日本航空電子工業株式会社内
(72)発明者　森　房夫
東京都渋谷区道玄坂１－21－２日本航空電子工業株式会社内
(72)発明者　石川　貢司
東京都渋谷区道玄坂１－21－２日本航空電子工業株式会社内
(72)発明者　大嶋　翼
東京都渋谷区宇田川町２－１渋谷ホームズ1205号株式会社駐車場綜合研究所内
(72)発明者　小島　雅夫
東京都あきる野市雨間563－１

Ｆターム(参考)　5B049 BB11 CC05 CC36 CC46 EE00 GG00 GG06